UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/975,815	10/11/2001	Neal A. Krawetz	10019968-1	9182

22879 7590 01/08/2009

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER
COLIN, CARL G

ART UNIT	PAPER NUMBER
2436	

NOTIFICATION DATE	DELIVERY MODE
01/08/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number: 09/975,815
Filing Date: October 11, 2001
Appellant(s): KRAWETZ, NEAL A.

James L. Baudino
Registration No. 43,486
For Appellant

EXAMINER'S ANSWER

This is in response to the appeal brief filed on October 10, 2008 appealing from the Office action mailed on June 12, 2008.

(1) Real Party in Interest

A statement identifying by name the real party in interest is contained in the brief.

(2) Related Appeals and Interferences

The examiner is not aware of any related appeals, interferences, or judicial proceedings which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(3) Status of Claims

The statement of the status of claims contained in the brief is correct.

(4) Status of Amendments After Final

The appellant's statement of the status of amendments after final rejection contained in the brief is correct.

(5) Summary of Claimed Subject Matter

The summary of claimed subject matter contained in the brief is correct.

(6) Grounds of Rejection to be Reviewed on Appeal

The appellant's statement of the grounds of rejection to be reviewed on appeal is correct.

(7) Claims Appendix

The copy of the appealed claims contained in the Appendix to the brief is correct.

(8) Evidence Relied Upon

6,931,128	ROBERTS	8-2005
6,751,736	BOWMAN ET AL	6-2004

(9) Grounds of Rejection

The following ground(s) of rejection are applicable to the appealed claims:

Claim Rejections - 35 USC § 112

9.1 The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-34 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The cited portion indicated by applicant page 8, lines 25-27, citing "*unlike secure shell and other tunneling protocols the encryption key changes with each transmitted data packet*" , which is the only section of the disclosure mentioning encryption key change and data packet, is not equivalent to the added limitations of the claims as amended. Applicant amends claim 1 to recite "generated a character string at a sender for each data packet associated with the secure data transmission"; "generating a hash key wherein the hash key is different for each data packet associated with the secure data transmission"… "encrypting a data packet associated with the secure data transmission". Applicant's specification page 8, lines 25-27 fails to provide support for these limitations in the claim. For instance, there is no description in the disclosure

for specifying which part of the encryption key changes for each data packet and there is no disclosure of data packet associated with the secure data transmission. Therefore, independent claims 1 and 19 are not supported by the original specification as amended. Claims 11 and 27 have been amended to recite "receiving plurality of character strings… receiving plurality of encrypted data packets each of the plurality of character strings correspond to one of the plurality of encrypted data packets… decrypting the plurality of encrypted data packets and the respective character strings. Neither one of these limitations is supported by the original specification as amended.

Claim Rejections - 35 USC § 102

9.2 The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-2, 4, 5, 7, 8, 11, 12, 14, 15, 19, and 22-25 are rejected under 35 U.S.C. 102(e) as being anticipated by US Patent 6,931,128 to **Roberts**.

As per claim 1, Roberts discloses a method for secure data transmission, comprising: generating a character string (seed) at a sender for each data packet associated with the secure data transmission (see column 3, lines 21-27);
generating a hash key using the character string (seed) and a private key (master secret) (see column 7, lines 34-67); wherein the hash key is different for each data packet associated with the secure data transmission (see column 10, lines 38-42) encrypting a data packet associated with the secure data transmission using the hash key (see column 9, lines 55-67); and transmitting an identification key (SPI) associated with the sender, the character string (seed), and the encrypted data packet from the sender to a recipient (see column 6, lines 45-54 and column 9, line 62 through column 10, line 5).

As per claim 2, Roberts discloses the limitation of wherein generating the hash key comprises hashing the character string (seed) with the private key (master secret) (see column 7, lines 34-67).

As per claim 4, Roberts discloses wherein generating a character string comprises randomly generating the character string (see column 7, lines 12-32).

As per claim 5, Roberts discloses determining the private key (master secret) at the recipient using the identification key (SPI) (see column 6, lines 45-54 and column 9, lines 58-

67); and decrypting the encrypted data at the recipient using the private key (master secret) and the character string (seed) (see column 10, lines 13-31).

As per claim 7, Roberts discloses determining the private key (master secret) at the recipient using the identification key (SPI) (see column 6, lines 45-54 and column 9, lines 58-67); determining the hash key at the recipient using the private key (master secret) and the character string (random seed) (see column 10, lines 13-31); decrypting the encrypted data using the hash key (see column 10, lines 13-31).

As per claim 8, Roberts discloses wherein determining the hash key comprises hashing the character string (random seed) with the private key (master secret) (see column 7, lines 34-67 and column 10, lines 18-21, stating the same procedure is performed at the decryption device).

As per claim 11, Roberts teaches a method for secure data transmission, comprising:
receiving a plurality of character strings (random seed) from a sender (see column 10, lines 37-42);
receiving an identification key (SPI) from the sender (see column 6, lines 45-54 and column 9, line 62 through column 10, line 5);
receiving a plurality of encrypted data packets from the sender each of the plurality of character strings correspond to one of the plurality of encrypted data packets (see column 10, lines 37-48 and column 11, lines 3-29; and column 13, lines 13-26);

determining a private key (master secret) associated with the sender using the identification key (SPI) (see column 6, lines 45-54 and column 9, lines 62-67); and decrypting the plurality of encrypted data packets using the private key (master secret) and the respective character strings (random seed) (see column 11, lines 3-29 and column 13, lines 13-26).

As per claim 12, Roberts discloses determining a hash key using the private key (master secret) and the character string (random seed) (see column 13, lines 13-26); and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key (see column 13, lines 13-26).

As per claim 14, Roberts discloses wherein receiving a character string (random string) comprises receiving a randomly generated character string (see column 7, lines 12-32).

As per claim 15, Roberts discloses hashing the character string (random seed) with the private key (master secret) to generate a hash key (see column 7, lines 34-67 and column 10, lines 18-21); and wherein decrypting the encrypted data comprises decrypting the encrypted data using the hash key (see column 10, lines 13-31).

As per claim 19, Roberts teaches a system for secure data transmission, (see fig. 1-2) comprising: a processor; a memory coupled to the processor (see fig.1); a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string (see column 4, lines 8-23 and column 7, lines 12-31); a hashing engine stored in

the memory and executable by the processor, the hashing engine adapted to generate a hash key using the character string (random seed) and a private key (master secret) (see column 7, lines 32-67) wherein the hash key is different for each data packet associated with the secure data transmission (see column 10, lines 38-48); an encryption engine stored in the memory and executable by the processor, the encryption engine adapted to encrypt the data using the hash key (see column 9, lines 55-67) and wherein the processor is adapted to transmit the encrypted data, an identification key (SPI) related to the private key (master secret), and the character string (random seed) to a recipient (see column 6, lines 45-54 and column 9, line 62 through column 10, line 5).

As per claim 22, Roberts discloses wherein the hashing engine is adapted to hash the character string (seed) with the private key (master secret) to generate the hash key (see column 7, lines 34-67).

As per claim 23, Roberts discloses wherein the string generator is adapted to randomly generate the character string (random seed) (see column 7, lines 12-32).

As per claim 24, Roberts discloses wherein the recipient is adapted to decrypt the encrypted data using the identification key (SPI) and the character string (random seed) (see column 6, lines 45-54 and column 9, lines 62-67) and (see column 11, lines 3-29 and column 13, lines 13-26).

As per claim 25, Roberts discloses wherein the recipient is adapted to determine the hash key using the identification key (SPI) and the character string (random seed) and decrypt the encrypted data using the hash key (see column 6, lines 45-54 and column 9, lines 62-67) and (see column 11, lines 3-29 and column 13, lines 13-26).

Claim Rejections - 35 USC § 103

9.3 The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 3, 6, 9, 10, 13, 16-18, 20-21, and 26-34 are rejected under 35 U.S.C. 103(a) as being unpatentable over US Patent 6,931,128 to **Roberts** in view of US Patent 6,751,736 to **Bowman et al.**

As per claim 3, Roberts does not explicitly disclose generating a signature using the hash key and the data and transmitting the signature to the recipient. **Bowman et al** in an analogous art discloses generating a signature using the secret string (private key) and the data

and transmitting the signature to the recipient (see column 7, lines 59-67). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a signature to protect the integrity of the data and transmitting the signature so that it can be verified at the other end to assure that they are identical as suggested by **Bowman et al** (see column 9, lines 50-55).

As per claim 6, Bowman et al discloses the limitation of wherein the recipient is adapted to access a relational database associating the identification key (secret ID) with the private key (secret sting) (see column 9, lines 27-29). Therefore, claim 6 is rejected on the same rationale as the rejection of claim 3 above.

As per claim 9, Roberts substantially discloses determining the hash key at the recipient using the private key (master secret) and the character string (random seed) (see column 10, lines 13-31); decrypting the encrypted data using the hash key (see column 10, lines 13-31). **Roberts** does not explicitly disclose generating a signature using the hash key and the data and transmitting the signature to the recipient. **Bowman et al** in an analogous art discloses generating a first signature by the sender using the secret string (private key) and the data and transmitting the first signature to the recipient (see column 7, lines 59-67). **Bowman et al** further discloses the recipient adapted to determine the hash key for decrypting the data and compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data (see column 9, lines 29-55). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a signature to protect the

integrity of the data and transmitting the signature so that it can be verified at the other end to assure that they are identical as suggested by **Bowman et al** (see column 9, lines 50-55).

As per claim 10, Roberts substantially discloses determining the private key (master secret) at the recipient using the identification key (SPI) (see column 6, lines 45-54 and column 9, lines 58-67); determining the hash key at the recipient using the private key (master secret) and the character string (random seed) (see column 10, lines 13-31); decrypting the encrypted data using the hash key (see column 10, lines 13-31). **Roberts** does not explicitly disclose generating a signature using the hash key and the data and transmitting the signature to the recipient. **Bowman et al** in an analogous art discloses generating a signature by the sender using the secret string (private key) and the data and transmitting the signature to the recipient (see column 7, lines 59-67). **Bowman et al** further discloses determining the private key (secret sting) at the recipient using the identification key (secret ID) (see column 9, lines 27-29); determining the hash key at the recipient using the private key (secret sting) and the character string (random string) (see column 9, lines 29-33); decrypting the encrypted data at the recipient using the hash key (see column 9, lines 33-35); and verifying the signature at the recipient using the hash key and the decrypted data (see column 9, lines 29-55). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash key instead of the private key to generate the signature for

better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a signature to protect the integrity of the data and transmitting the signature so that it can be verified at the other end to assure that they are identical as suggested by **Bowman et al** (see column 9, lines 50-55).

As per claim 13, Bowman et al discloses wherein determining the private key comprises accessing a relational database associating the identification key (secret ID) with the private key (secret sting) (see column 9, lines 27-29). Therefore, claim 13 is rejected on the same rationale as the rejection of claim 10 above.

As per claim 16, Bowman et al discloses receiving a signature from the sender (see column 7, lines 59-67); and verifying the signature using the decrypted data, the private key (secret sting), and the character string (random string) (see column 9, lines 29-55). Therefore, claim 16 is rejected on the same rationale as the rejection of claim 10 above.

As per claim 17, Bowman et al discloses receiving a signature from the sender (see column 7, lines 59-67), determining a hash key using the private key (secret sting) and the character string (random string) (see column 9, lines 29-33); and verifying the signature using the decrypted data and the hash key (see column 9, lines 29-55). Therefore, claim 17 is rejected on the same rationale as the rejection of claim 10 above.

As per claim 18, Roberts substantially discloses determining the hash key at the recipient using the private key (master secret) and the character string (random seed) (see column 10, lines 13-31). **Roberts** does not explicitly disclose generating a second signature using the hash key and the decrypted data and comparing the signatures. **Bowman et al** in an analogous art discloses receiving a first signature from the sender (see column 7, lines 59-67); determining the hash key at the recipient using the private key (secret sting) and the character string (random string) (see column 9, lines 29-33); generating a second signature by the sender using the secret string (private key) and the decrypted data (see column 9, lines 33-50); and comparing the first signature to the second signature (see column 9, lines 43-50). **Bowman et al** further discloses the recipient adapted to determine the hash key for decrypting the data and compare the first signature to a second signature generated by the recipient using the hash key and the decrypted data (see column 9, lines 29-55). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash

key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a signature to protect the integrity of the data and transmitting the signature so that it can be verified at the other end to assure that they are identical as suggested by **Bowman et al** (see column 9, lines 50-55).

As per claim 20, Roberts does not explicitly disclose generating a signature using the hash key and the data and transmitting the signature to the recipient. **Bowman et al** in an analogous art discloses a signature engine (hash algorithm) stored in the memory and executable by the processor, (see column 13, lines 10-39) the signature engine adapted to generate a signature using the secret string (private key) and the data, the processor further adapted to transmit the signature to the recipient (see column 7, lines 59-67). The difference between **Bowman et al** and the claimed invention is that Bowman et al uses the private key to generate the signature whereas the claimed invention uses the hash key. **Bowman et al** teaches the hash key is generated from the secret string (private key) and a random string (see column 7, lines 29-41), therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to use the hash key instead of the private key to generate the signature for

better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as suggested by **Bowman et al** it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a signature to protect the integrity of the data and transmitting the signature so that it can be verified at the other end to assure that they are identical as suggested by **Bowman et al** (see column 9, lines 50-55).

As per claim 21, Bowman et al discloses wherein the recipient is adapted to decrypt the encrypted data and verify the signature using the decrypted data (see, column 9, lines 33-55). Therefore, claim 21 is rejected on the same rationale as the rejection of claim 20 above.

As per claim 26, Bowman et al discloses the limitation of wherein the recipient is adapted to access a relational database associating the identification key (secret ID) with the private key (secret sting) (see column 9, lines 27-29). Therefore, claim 26 is rejected on the same rationale as the rejection of claim 20 above.

As per claim 27, Roberts substantially discloses a system for secure data transmission, (see fig. 11) comprising: a processor adapted to receive a plurality of encrypted data packets, an

identification key (SPI), and a plurality of character strings (random seed) from a sender, each of the plurality of character strings correspond to one of the plurality of encrypted data packets (see column 11, lines 3-29 and column 13, lines 13-26); a memory coupled to the processor (see fig.1); a decryption engine stored in the memory and executable by the processor, the decryption engine adapted to decrypt the encrypted data packets using the respective character strings (random seed) and the private key (master secret) (see column 4, lines 8-23 and column 10, lines 13-31). **Roberts** does not explicitly disclose a relational database stored in the memory and accessible by the processor, the relational database relating the identification key to a private key. **Bowman et al** in an analogous art discloses a relational database stored in the memory and accessible by the processor, the relational database relating the identification key (secret ID) to a private key (secret sting) (see column 9, lines 27-29). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify **Roberts** to use a relational database because it would make it easier to select the corresponding private key to generate the encryption key as suggested by **Bowman et al** (see column 9, lines 27-29).

As per claim 28, the references as combined above disclose a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the character string (random seed) and a private key (master secret) and the decryption engine adapted to decrypt the encrypted data using the hash key (see **Roberts**, column 7, lines 32-67) and (see **Roberts**, column 11, lines 3-29 and column 13, lines 13-26). (See also **Bowman et al** column 9, lines 29-35)

As per claim 29, the references as combined above disclose comprising a signature engine (hash algorithm) stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the private key (secret sting), and the character string (random string) (see **Bowman et al** column 9, lines 29-55). Therefore, claim 29 is rejected on the same rationale as the rejection of claim 27 above.

As per claim 30, the references as combined above disclose a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to generate a hash key using the private key (secret sting), and the character string (random string) (see **Bowman et al** column 9, lines 29-55); and a signature engine stored in the memory and executable by the processor, the signature engine adapted to verify a signature received from the sender using the hash key and the decrypted data (see **Bowman et al** column 9, lines 29-55). Therefore, claim 30 is rejected on the same rationale as the rejection of claim 27 above.

As per claim 31, the references as combined above disclose a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to hash the character string (random seed) with the private key (master secret) and the decryption engine adapted to decrypt the encrypted data using the hash key (see **Roberts**, column 7, lines 32-67) and (see **Roberts**, column 11, lines 3-29 and column 13, lines 13-26) (see **Bowman et al** column 9, lines 29-35).

As per claim 32, the references as combined above disclose a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string (random seed) and wherein the decryption engine is further adapted to encrypt data for transmitting to the sender using the character string (random seed) and the private key (master secret) (see **Roberts**, column 7, lines 12-32 and column 11, lines 3-29 and column 13, lines 13-26) (see **Bowman et al** column 7, lines 25-29; column 9, lines 29-55 and column 11, line 65 through column 12, line 14).

As per claim 33, the references as combined above disclose a string generator stored in the memory and executable by the processor, the string generator adapted to generate a character string; a hashing engine stored in the memory and executable by the processor, the hashing engine adapted to hash the character string with the private key to generate a hash key; and wherein the decryption engine is further adapted to encrypt data for transmitting to the sender using the hash key (see **Roberts**, column 7, lines 12-32 and column 11, lines 3-29 and column 13, lines 13-26) (see **Bowman et al** column 7, lines 25-29; column 9, lines 29-55 and column 11, line 65 through column 12, line 14).

As per claim 34, Bowman et al discloses a signature engine stored in the memory and executable by the processor, the signature engine adapted to generate a first signature using the decrypted data and compare the first signature to a second signature received from the sender (see column 9, lines 29-55). Therefore, claim 34 is rejected on the same rationale as the rejection of claim 27 above.

(10) Response to Argument

10.1 Appellant's arguments, see pages 4-18, in the appeal brief filed on 10/10/2008 with respect to claims 1-34 are not persuasive.

Regarding the 35 USC 112th first paragraph, it appears that appellant argues that the rejection requirements by the Examiner are not met, citing sections of the MPEP § 2163.04. Examiner respectfully disagrees as the rejection made by the Examiner identifies the claim limitation(s) at issue and the rejection establishes a prima facie case by showing that the support for the limitation is not apparent and the citation provided by appellant for support is not sufficient for pointing out where the limitation is supported as stated in the MPEP § 2163.04 (I).

See MPEP § 2163.04 (I)

In rejecting a claim, the examiner must set forth express findings of fact which support the lack of written description conclusion (see MPEP § 2163 for examination guidelines pertaining to the written description requirement). These findings should:

*(A) Identify the claim *>limitation(s)< at issue; and*

(B) Establish a prima facie case by providing reasons why a person skilled in the art at the time the application was filed would not have recognized that the inventor was in possession of the invention as claimed in view of the disclosure of the application as filed. A general allegation of "unpredictability in the art" is not a sufficient reason to support a rejection for lack of adequate written description. A simple statement such as "Applicant has not pointed out where the new (or amended) claim is supported, nor does there appear to be a written description of the claim limitation ____' in the application as filed." may be sufficient where

the claim is a new or amended claim, the support for the limitation is not apparent, and applicant has not pointed out where the limitation is supported. > See Hyatt v. Dudas, 492 F.3d 1365, 1370, 83 USPQ2d 1373, 1376 (Fed. Cir. 2007) (holding that "[MPEP] § 2163.04 (I)(B) as written is a lawful formulation of the prima facie standard for a lack of written description rejection.").<

Appellant describes the invention in the application as filed in terms of **data** being transmitted (as a **general term**). As amended, Appellant relies on page 8, lines 25-27 (see applicant's arguments, page 8, filed on 2/19/2008), citing "*unlike secure shell and other tunneling protocols the encryption key changes with each transmitted data packet*", to **narrow** the claim limitations to a data packet, plurality of character strings, plurality of data packets, corresponding data packet and string, and also to each data packet associated with secure data transmission.

For instance, **regarding claim 1,** the following amended limitations in claim 1:

"*generating a character string for each data packet associated with secure data transmission; wherein the hash key is different for each data packet associated with secure data transmission; encrypting a data packet associated with secure data transmission; transmitted an identification key associated with the sender, the character string, and the encrypted data packet from the sender to a recipient*"

do not appear to be supported by only page 8, lines 25-27 written description as-filed nor this section pointed out by applicant is sufficient. Thus, they are not supported in the original specification through express, implicit, or inherent disclosure.

Regarding the limitation of generating a character string for each data packet associated with secure data transmission;

Appellant cites (See appeal brief, page 2, Summary of Claimed Subject Matter),

generating a character string (Pg. 4, lines 19-20; pg. 7, lines 18-19; Fig. 2, Ref. 208). at a sender (Pg. 3, lines 22-24; Fig. 1, Ref. 18) for each data packet associated with the secure data transmission (Pg. 8, lines 25-27; Fig. 2),

Page 4, lines 19-20 as reproduced below cites,

"*In operation, the string generator 40 randomly generates and stores the character string 54 in the database 50. The hashing engine 42 hashes the character string 54 with the private key 62 to generate the hash key 64, which is also stored in the database 50.*"

Page 7, lines 18-19 and ref. 208 is reproduced below:

"At step 208, the string generator 40 generates a random character string 54 and stores the character string 54 in the database 50."

Page 8, lines 25-27 is reproduced below:

"*Further, unlike secure shell or other tunneling protocols, the encryption key changes with each transmitted data packet, thereby further reducing the likelihood of third party interception and subversion.*"

Appellant argues (see end of page 6 to page 7),

On page 8, in lines 25-27, of the originally-filed disclosure, Appellant states that "unlike secure shell or other tunneling protocols, the encryption key changes with each transmitted data packet" (emphasis added). As disclosed on page 4, lines 20-22, and illustrated in block 210 of Fig. 2, the encryption key (a.k.a., the hash key 64) is generated using the character string 54 and the private key 62. Appellant submits that one skilled in the art would recognize that the variable used to generate the hash key 64, namely the character string 54, is changed to generate a hash key 64 that "changes with each transmitted, data packet" as expressly disclosed on page 8, in lines 25-27, of the originally-filed disclosure. For example, at least on page 4 of the originally-filed disclosure, it is stated that "the string generator randomly generates and stores the character string," and that the character string is hashed with. the private key to generate the hash key (page 4, lines 19-33). Moreover, one skilled in the art would recognize that the encrypted data packets are associated with the secure transmission.

As shown above, the application as filed which disclosed a *hash key 64* generated from two sets of data (*character string 54 with the private key 62*) and also disclosed the encryption key changes with each transmitted data packet did not specifically disclose generating a character string for each data packet associated with secure data transmission. Note that Appellant's statement "***the variable*** *used to generate the hash key 64,* ***namely the character string 54***" is not correct because the hash key is dependent upon two variables named (*the character string 54 and the private key 62*). The fact that the encryption key changes with each transmitted data packet does not inherently or implicitly mean a character string is generated for each data packet associated with the secure data transmission because a change in the encryption key even when assuming it is the hash key can be caused by any of the two sets of data or by none of them (i.e. other means by adding salt to the encryption key). Note also that Appellant states "*the character string is changed to generate a hash key that changes with each transmitted data packet as expressly disclosed on page 8, lines 25-27 of the originally-filed disclosur*e". Examiner respectfully disagrees with appellant's statement. Such disclosure is not expressly disclosed on page 8, lines 25-27. In addition, the character string is not described in the specification as filed as being generated for each data packet associated with the secure data transmission. On the other hand, the original specification describes one character string being generated and stored in the database and the whole disclosure is described specifically according to that randomly generated character string 64 stored in the database of the client and the same character string 64 received by the server from the client and stored as a character string 116 in the server database (see specification page 6, lines 5-6). Appellant has not pointed out where the

amended character string that changes to generate a hash key that changes with each transmitted data packet is supported nor does there appear to be a written description of it on page 8, lines 25-27. Therefore, claim 1 contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Regarding claims 11, 19, and 27, **Appellant** on page 7 **mentions** that **the amendments to independent claims 11, 19, and 27 are also supported for the same reason with respect to claim 1**. Examiner respectfully disagrees for at least the reasons mentioned above with respect to claim 1.

In addition, Appellant has not pointed out where other amended claim 11 limitations *"receiving a plurality of character strings from a sender; receiving a plurality of encrypted data packets from the sender, each of the plurality of character strings correspond to one of the plurality of encrypted data packets; decrypting the plurality of encrypted data packets using the respective private key and the respective character strings"* are supported nor does there appear to be a written description of the claimed limitations.

In the summary of claimed subject matter, **with respect to claim 11**, appellant cites,

receiving a plurality of character strings from a sender (Pg. 7, line 31; Pg. 8, lines 1-2, 25-27; Fig. 3. Ref. 304), receiving an identification key from the sender (Pg. 7, line 31; Pg. 8, lines 1-2; Fig. 3. Ref. 304), receiving a plurality of encrypted data packets from the sender (Pg. 7, line 31; Pg. 8, lines 1-2; Fig. 3. Ref. 304), each of the plurality of character strings correspond to one of the plurality of encrypted data packets (Pg. 8, lines 25-27; Fig. 3),

Page 7, line 31 through page 8, line 2 is reproduced below:

"At step 304, the server 20 receives ***the character string*** *54, the encrypted data 72, the identification key 60 corresponding to* ***the transmitting client 18****, and the signature 56 from the client 18."*

Page 8, lines 25-27 is reproduced below:

"*Further, unlike secure shell or other tunneling protocols,* ***the encryption key*** *changes with each transmitted data packet, thereby further reducing the likelihood of third party interception and subversion."*

It does not appear to be a written description for the amended claimed limitations nor does the original specification provides support for the amended limitations through express, implicit, or inherent disclosure. Limitations with respect to plurality of character strings and plurality of data packets received from a sender, each of the plurality of encrypted data packets corresponding to each of the plurality of character strings were not supported by the original patent's disclosure in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

For at least the reasons mentioned above, claims 19 and 27 reciting similar limitations with respect to claims 1 and 11 and the intervening claims dependent from claims 1, 11, 19, and 27 should remain rejected under 35 USC 112 first paragraph.

10.2 With regard to the prior art rejection of claim 1, **Appellant argues**, see pages 7-8, that **Roberts appears to disclose transmitting an identification key (SPI) associated with the recipient (the second computer system) and does not appear to be associated with the sender (first computer system)**, relying on column 9, line 65 through column 10, line 7.

Examiner respectfully disagrees as Roberts clearly discloses, see column 6, lines 45-54, both the first and second computer systems negotiate a master secret key that is to be known by only (unique to) the first and second computer systems and a security parameter index (SPI) associated with the master secret is also negotiated. Therefore, the SPI is associated with the sender or first computer system. Column 13, lines 15-30 further discloses the SPI is included in the received data packets from the first computer system. Therefore, Roberts discloses transmitting an identification key (SPI) associated with the sender as claimed in claim 1. In addition, Roberts discloses an identifying label for generating a key at the sender that meets the recitation of an identification key associated with the sender (see column 7, lines 45-55), the label is concatenated with the random seed and transmitted to the second computer system (see column 9, lines 45-50 and 62-63) that also meets the claimed recitation of transmitting an identification key associated with the sender. For the sake of argument, Roberts disclosing the first and second computer negotiating a parameter expiry identifying the valid lifetime of the master secret (see column 10, lines 53-59 and column 6, lines 45-54) that also meets the claimed recitation of an identification key associated with the sender. Therefore, contrarily to Appellant's arguments that Roberts' identification key appears to be associated with the second computer system (the receiving computer) and not to the sender (first computer system), Examiner respectfully asserts that Roberts discloses identification key being associated with both the first and the second computer system as shown above.

Claims 2, 4, and 8 which depend either directly or indirectly upon claim 1 are not separately argued by Appellant, and therefore, they are not patentable for at least the reasons given above with respect to claim 1.

Regarding claims 5 and 7, **Appellant states**, see page 9, "***Appellant is unable to locate any teaching or suggestion in Roberts that the Secure Parameter Index (SPI) is used in determining the private key at the recipient using the identification key***." Examiner respectfully disagrees as an identification key is implicitly used to identify a key and the SPI is by definition an identification tag added to the header of the data packet to determine which encryption algorithms and rules to use; in this case, the master secret is a symmetric key wherein the same key is used by both the sender and the recipient (see column 6, lines 45-54 and column 7, lines 2-5). Thus, at the recipient side, the master secret is determined using the identification tag (SPI). In addition, Roberts discloses an identifying label for generating a key at the sender (see column 7, lines 45-55), the label is concatenated with the random seed and transmitted to the second computer system (see column 9, lines 45-52 and 62-63). Thus, the random seed, which includes the identifying label is used to generate a key (see column 13, lines 6-30). Note that as disclosed in column 13, lines 6-30, each data packet is encrypted with a different key based on the random seed. The second computer system needs to determine the key by reading the at least the random seed to generate the key to decrypt the data packet. Therefore, the rejection of claims 5 and 7 should be sustained.

Regarding claims 11, 12, and 14-15, Appellant presents the same arguments with respect to claims 1, 5 and 7. Therefore, the rejection of these claims should be sustained in view of the response to arguments made with respect to claims 1, 5 and 7 above.

Regarding claims 19, and 22-24, Appellant argues with respect to claim 19 that Roberts does not disclose an identification key related to the private key. Appellant presents the same arguments with respect to claim 1. Therefore, the rejection of these claims should be sustained in view of the response to arguments made with respect to claim 1 above.

Regarding claim 25, **Appellant states**, see page 11, "***Appellant is unable to locate any teaching or suggestion in Roberts that the Secure Parameter Index (SPI) is useable by the recipient to determine the hash key.***" Examiner respectfully disagrees as an identification key is implicitly used to identify a key and the SPI is by definition an identification tag added to the header of the data packet to determine which encryption algorithms and rules to use; in this case, the master secret is a symmetric key wherein the same key is used by both the sender and the recipient (see column 6, lines 45-54 and column 7, lines 2-5). Thus at the recipient side, the master secret is determined using the identification tag (SPI). In addition, Roberts discloses an identifying label for generating a key at the sender (see column 7, lines 45-55), the label is concatenated with the random seed and transmitted to the second computer system (see column 9, lines 45-52 and 62-63). Thus, the random seed, which includes the identifying label is used to generate a hash key (see column 7, lines 45-55). The same procedure is used at the receiving side (see column 13, lines 6-30). Note that as disclosed in column 13, lines 6-30, each data

packet is encrypted with a different key based on the random seed. The second computer system needs to determine the key by reading the at least the random seed to generate the key to decrypt the data packet. Therefore, the rejection of claim 25 should be sustained.

Regarding claim 27, **Appellant states**, see pages 11-12, "***Appellant is unable to locate any teaching or suggestion in Roberts that the Secure Parameter Index (SPI) is employed as an identification key as recited in claim 27 much less an identification key identifying a particular client as defined in the originally-filed specification.***" Examiner respectfully disagrees as an identification key is implicitly used to identify a key and the SPI is by definition an identification tag added to the header of the data packet to determine which encryption algorithms and rules to use; in this case, the master secret is a symmetric key wherein the same key is used by both the sender and the recipient (see column 6, lines 45-54 and column 7, lines 2-5). In addition, Roberts discloses an identifying label for generating a key at the sender that meets the recitation of an identification key associated with the sender (see column 7, lines 45-55), the label is concatenated with the seed and transmitted to the second computer system (see column 9, lines 45-50 and 62-63).

Bowman even discloses a secret ID related to a secret string that meets the recitation of identification key related to a private key, (see column 9, lines 11-33) as reproduced below:

"**A secret ID 673**, **is supplied** and is concatenated in block 680 with the random string, 670, and the encrypted message string, 649. The concatenated string is character encoded, preferably, Base64 encoded in block 683, and the resulting VBC, 685 is then formatted in an HTML document, in block 687 as discussed above.

(40) Referring to FIG. 7 an algorithm for decoding, decrypting, and authenticating the VBC produced by the algorithm

of FIG. 6 is represented. In block 711 VBC is received after being parsed from a received HTTP message, which may include selected option name value pairs. In block 714, the received VBC is decoded (e.g., base 64 decoded) to produce a binary string from received character string, and in block 717 the binary string is parsed to separate the encrypted string, 721, the random sting, 724, and the secret ID 727. **The secret ID is used as an index into a database in block 730 to access the corresponding secret string, 733**. The secret string, 733 is concatenated in block 736 with the random string, 724. The result is supplied to a key generating secure hash algorithm in block 739, which produces a SHAD 742 (identical to 640 in FIG. 6), which is used as the decryption key."

In response to Appellant's arguments that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the identification key 60 may comprise a serial number or other type of identifier indicating the particular client 18 transmitting the data (see brief, last paragraph of page 11), and identification key identifying a particular client as defined in the originally-filed specification (see brief page 12)) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

Appellant further argues that the combination of Roberts and Bowman is not proper because

"Roberts appears to disclose that the master secret is negotiated between the first and second computers prior to the commencement of any secure communications. Appellant submits that the exchange of the master secret of Roberts outside of secure communications avoids the possibility that the master secret, which is used to decrypt the encrypted information, could be intercepted at the same time as the encrypted information during transmission."

Examiner respectfully disagrees as Roberts discloses the SPI is included in the data packet (see column 11, lines 34-36), and also discloses the identifying label concatenated with the random seed is included in the data packet (see column 7, lines 45-55; column 9, lines 45-51

and column 10, lines 13-15). Examiner asserts that contrarily to appellant's interpretation Roberts also discloses sensitive information transmitted along with the data packet. Appellant's reasoning that the negotiation of the master secret is what avoids the possibility that the master secret could be intercepted is not well founded as Roberts discloses to avoid the possibility of the master secret and the key to be identified by eavesdroppers, a key is generated using the master secret and a seed (see column 7, lines 5-11) and also discloses using hash functions for increased security (see column 7, lines 52-55), and further discloses the seed used to generate the key contains a random bit sequence, makes it even more difficult to identify the key or master secret to thereby be able to intercept a sensitive message (see column 10, lines 32-37); and to say the least, Roberts discloses a new random bit sequence is even generated for each data packet (see column 10, lines 38-48). Therefore, Appellant's arguments that because the secret ID is transmitted along with the encrypted VBC, one skilled in the art would not look to combine Roberts with Bowman do not appear to be well-founded. Note that the secret ID of Bowman is not even transmitted in the clear (see figure 4).

Claims 28-34, which depend either directly or indirectly upon claim 27 are not separately argued by Appellant, and therefore, the rejection with respect to claims 28-34 should be sustained in view of the response to arguments made in claim 27 above.

Regarding claims 3, 10, and 20, **Appellant states** that **Bowman does not appear to teach a signature because Appellee has not specifically pointed out and Appellant is unable to determine a signature in the quoted portion column 7, lines 59-67**. Examiner directs

Appellant to the other quoted portion in column 9, lines 50-55 disclosing that a signature 765 is being calculated at the receiver to verify the signature 755 received from the sender. In the rejection of claim 10, it is disclosed cited portions of column 9, lines 29-55 for verifying the signature at the recipient. Therefore, Appellant was aware that other portions in the reference discloses a signature. Examiner made a typing error writing column 7, lines 59-67 instead of column 8, lines 59-67.

Column 8, lines 59-67 cites,

Referring to FIG. 6, a flow diagram of an algorithm for generating a signed, encrypted and encoded VBC is shown. Field name value pairs of product descriptors are provided in block 610. In block 614 the field name value pairs are concatenated with appropriate delimiters to produce the VBC message data 615 string. A secret string is provided in block 631. **The secret string is concatenated with VBC message data in block 618. The resulting concatenated string is supplied as input to a signature secure hash algorithm in block 621. The secure hash algorithm generates a signature SHAD 624**. The signature SHAD is used to authenticate the VBC message data at the ultimate destination.

Therefore, Examiner asserts that Bowman does disclose generating a signature using the private key (secret string) and the data. Concerning Appellant's arguments (see brief, page 14, last paragraph through page 15) about Examiner's statement that one of ordinary skill in the art would favor the hash key instead of the private key, Examiner asserts that there is enough

teaching and suggestion of the prior art in addition to the knowledge of one of ordinary skill in the art to recognize the advantage to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see Bowman column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as Bowman suggested that it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55), thus hashing the key as taught by Roberts would have made it more difficult to an unlawful party to know the key as Roberts discloses using a hash for better security (see column 7, lines 52-55).

For at least the reasons above, the rejection of claims 3, 10, and 20 should be sustained.

Regarding claim 9, Appellant states,

"Appellee has not specifically pointed out, and Appellant is unable to determine, where a "first signature"as recited in Claim 9 is included in the cited portion of Bowman, much less a "second signature." Moreover, Appellee has not specifically pointed out, and Appellant is unable to determine, where "data" as recited in Claim 9 is included in the cited portion of Bowman. As noted above, according to 37 C.F.R. §1.104(c)(2), the pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified."

Examiner respectfully disagrees as the cited portion of Bowman, column 9, lines 29-55, clearly discloses a signature 765 is being calculated at the receiver to verify the signature 755 (624 in fig. 6) received from the sender. Therefore, signature 755 (624 in fig. 6) is clearly the first signature and 765 is clearly the second signature.

See also column 14, lines 22-44 which cites,

"3. The communication method of claim 1, wherein the step of concatenating at least a plurality of descriptors to form a

first string comprises: concatenating the plurality of descriptors and a secret string to produce a descriptor-secret string; **applying a signature secure hash algorithm digest to the descriptor-secret string to produce a first signature**; and concatenating the first signature with the plurality of descriptors to produce the first string.

4. The communication method of claim 3 further comprising: parsing the first string on the second server to separate the first signature from the plurality of descriptors; concatenating the secret string with the plurality of descriptors to produce the descriptor-secret string on the second server; **applying the signature secure hash algorithm to the descriptor-secret string to produce a second signature on the second server; and comparing the first signature to the second signature**; whereby the authenticity of the encrypted string can be determined."

Therefore, there is clearly disclosure in Bowman of first and second signatures.

Concerning Appellant's arguments (see brief, page 16) about Examiner's statement that one of ordinary skill in the art would favor the hash key instead of the private key, Examiner asserts that there is enough teaching and suggestion of the prior art in addition to the knowledge of one of ordinary skill in the art to recognize the advantage to use the hash key instead of the private key to generate the signature for better security since it is harder for the recipient to be in possession of the hash key that needs to be regenerated using the secret string (private key) than it is for the recipient to determine the secret string (private key) (see Bowman column 8, lines 35-45); One of ordinary skill in the art would have recognized this advantage for using the hash key instead of the private key as Bowman suggested that it only requires an unlawful party to know the key that was used by the sender to duplicate the signature (see column 9, lines 50-55), thus hashing the key as taught by Roberts would have made it more difficult to an unlawful party

to know the key as Roberts discloses using a hash for better security (see Roberts, column 7, lines 52-55).

For at least the reasons above, the rejection of claim 9 should be sustained.

Regarding claims 16 and 17, **Appellant argues** that **Bowman does not appear to teach receiving a signature from a sender**. Examiner respectfully disagrees and directs Appellant to column 8, lines 59-67disclosing the sender's signature used for authentication at the ultimate destination (target computer). Column 9, lines 29-55, clearly discloses a signature 765 is being calculated at the receiver to verify the signature 755 (624 in fig. 6) received from the sender.

Claims 6, 13, 18, 21, 26, and 28, which depend either directly or indirectly upon claims 1, 11, 19, and 27 are not separately argued by Appellant, and therefore, the rejection with respect to claims 6, 13, 18, 21, 26, and 28 should be sustained in view of the response to arguments made in claims 1, 11, 19, and 27 above.

(11) Related Proceeding(s) Appendix

No decision rendered by a court or the Board is identified by the examiner in the Related Appeals and Interferences section of this examiner's answer.

For the above reasons, it is believed that the rejections should be sustained.

Respectfully submitted,

/Carl Colin/
Primary Examiner, Art Unit 2436
December 30, 2008

Conferees:

Nasser Moazzami

/Nasser G Moazzami/

Supervisory Patent Examiner, Art Unit 2436

Kim Vu

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435

Hewlett-Packard Development Company, LP,
20555 S.H. 249
Houston, TX 77070, U.S.A.